



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/989,883	11/21/2001	Philippe Stransky	16674-6	1499
7590	01/18/2007		EXAMINER	
Clifford W. Browning Woodard, Emhardt, Naughton, Moriarty & McNett Bank One Center/Tower 111 Monument Circle, Suite 3700 Indianapolis, IN 46204-5137			SHIFERAW, ELENI A	
			ART UNIT	PAPER NUMBER
			2136	
SHORTENED STATUTORY PERIOD OF RESPONSE		MAIL DATE	DELIVERY MODE	
3 MONTHS		01/18/2007	PAPER	

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	Application No.	Applicant(s)
	09/989,883	STRANSKY ET AL.
	Examiner	Art Unit
	Eleni A. Shiferaw	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 27 October 2006.
- 2a) This action is FINAL.                            2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-6 is/are pending in the application.
  - 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-6 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.
 

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) All    b) Some \* c) None of:
    1. Certified copies of the priority documents have been received.
    2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)	5) <input type="checkbox"/> Notice of Informal Patent Application
Paper No(s)/Mail Date _____	6) <input type="checkbox"/> Other: _____

**DETAILED ACTION**

***Response to Amendment/Arguments***

1. Applicant's arguments with respect to claims 1-6 have been considered but are moot in view of the new ground(s) of rejection.
2. Claims 1-6 are pending.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challender et al. USPN 6,959,390 B1 in view of Matyas, Jr. et al. USPN 6,947,556 B1 and Hind et al. USPN 6,980,660 B1.

Regarding claim 1, Challener et al. teaches a method of production and distribution of asymmetric public and private keys to provide certifications of transactions (fig. 4), comprising the steps of:

providing a key generation center in charge of generating a plurality of asymmetric public and private keys to be used to provide certificates of transactions (fig. 4 element 402 and 408; *plurality of private/public keys is generated for certifications*),

generating certificates comprising a public key and a private key in a first cryptographic unit (KPG) of the key generation center (claim 6 and col. 3 lines 17-31),  
coding the private key by means of a service key in the key generation center in the first cryptographic unit (KPG) (col. 2 lines 59-67; *encrypting private key of the user using master public key of the key generator*) and storing said coded private key in a key memory (KPS) of the key generation center (claim 1; *encrypting user's private keys and storing encrypted keys*),

when preparing to send the public and private keys to a user unit, extracting the keys from the key memory (KPS), and composing the certificates with the public key (col. 3 lines 17-31, and claim 1; *extracting the keys from storage to be transmitted to users and attaching certificate for user's application to access the keys*),

decoding the corresponding private key by means of a service key in a cryptographic security module and coding it with a transport key of the user (claim 1 and 6; *encrypted keys are extracted, decrypted using master private key, and encrypted using user's public key*).

Challender et al. discloses coding the private key by means of a public master key. Challender et al. fails to disclose encrypting the private key by means of secret service key.

However Matyas, JR. et al. discloses the well-known encryption of private key encrypting key method (col. 1 lines 53-col. 2 lines 58; *encrypting the first key with the second personal key and further encrypting the first key with control key...*).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of Matyas, Jr. et al. with in the system of Challender et al. because they are analogous in key management. One would have been

motivated to do so because it would further secure key by encrypting keys using a well-known method of private key.

The combination of Challender et al. and Matyas, JR. et al. disclose generating a master key pair (pub/priv key pair), and generating a unique user key pair for plurality of users, and encrypting each users pub/private key pairs using master public key/personal key and storing master public key in a protected storage and storing encrypted user key pairs in unsecured storage securely (Challender et al. abstract, and Matyas, Jr. et al. col. 1 lines 53-col. 2 lines 58). When a user requests an application, the encryption engine decrypts the encrypted user key pairs to encrypt message (see Challender et al. claims 1-2). *The generated user private public key pairs are accessed by an application of a user's system* (Challender et al. col. 3 lines 10-16). The combination fails to explicitly disclose transmitting the public key and the encrypted private key to a user unit. However Hind et al. discloses a server generating a public/private key pair and associated certificate for the enterprise device and securely transmits these generated data items to the device for which they were generated (see col. 8 lines 56-67).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Hind et al. with in the combination system because they are analogous in cryptography. One would have been motivated to do so because it is obvious to transmit both private key and public key to user's device after generating the pairs.

Regarding claim 2, Hind et al. discloses a method characterized in that the encrypted private key is received by the user unit (DEC) and transmitted to the security module (SM) containing the transport key for decoding and storing the private key (col. 8 lines 23-24). It would have been

obvious to one having ordinary skill in the art at the time of the invention was made to store the user's private key in the user's device because it is private to the user and the user can use it to decrypt data.

Regarding claim 3, Challender et al. further discloses teaches a method characterized in that it comprises in using several monolithic cryptographic unit to obtain a high speed coding module (col. 5 lines 5-41).

5. Claims 4-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challender et al. USPN 6,959,390 B1 in view of Matyas, Jr. et al. USPN 6,947,556 B1, and Hind et al. USPN 6,980,660 B1, and further in view of Tarpenning et al. USPG PUB 2002/0007454 A1.

Regarding claims 4, 5, and 6, Challender et al., Matyas, JR. et al., and Hind et al. teach all the subject matter as described above. Challender et al., Matyas, JR. et al., and Hind et al. fail to explicitly disclose coding the public key of the center with the transport key, transmitting it to user unit, receiving it at the user unit, decoding and it at the user unit.

However Tarpenning et al. teaches a method characterized in that it comprises in:  
coding the public key of the center with the transport key and transmitting it to the user unit (DEC) (0032),  
receiving by the user unit, the encrypted public key and transmitting it to the security module (SM) (fig. 2),

decoding and storing the public key by means of the transport key inside the security module (SM) (0033).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of encrypting the public key of the center using the user's public key/transport key within the combination system because they are analogous in generation of keys and certificates. One would have been motivated to incorporate the teachings of Tarpenning et al. within the combination system because it would allow secure authentication of users identity.

***Conclusion***

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

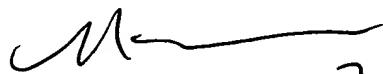
Art Unit: 2136

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



January 11, 2007

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

  
1/11/07